IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

IN RE: TAASERA LICENSING LLC, PATENT LITIGATION	§ § § §	Case No. 2:22-md-03042-JRG **JURY TRIAL DEMANDED**
THIS DOCUMENT RELATES TO ALL ACTIONS	§ § § §	

TAASERA LICENSING LLC'S
REPLY CLAIM CONSTRUCTION BRIEF

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

I. DISPUTED CLAIM TERMS

1. "regularly identifiable expression" / "regular expression" (Claim 1, '796 Patent)

Taasera agrees to construe this term according to the plain and ordinary meaning.

2. "if the new program is validated, permitting the new program to continue loading and to execute in connection with the computing device" (Claims 6, 13, 14, and 24, '137 Patent)

The parties' dispute rests on (i) whether monitoring can occur even "if the new program is validated;" and (ii) whether monitoring is relevant to the language of this specific claim limitation, which only describes "permitting the new program to continue loading and to execute." Defendants acknowledge Taasera's citation to the specification, which unequivocally shows that a validated program may still be monitored (either minimally or not at all), as it continues loading and executes. Dkt. 259, 5; *See* Ex. B, 3:49-62. Defendants' construction cannot improperly nullify a disclosed embodiment, even if it is only disclosed in "a single passage." Dkt. 259, 4-5. Defendants then argue that Plaintiff must provide a construction because "Plaintiff fails to explain what the phrase 'little… additional security monitoring' means" in this embodiment. But this is not the claim language, and Taasera does not need to construe terms in the specification. What is clear is the claim language, which describes that "if the new program is validated, permitting the new program to continue loading and to execute." Monitoring is only required in another claim limitation ("***if the new program is not validated***, ***monitoring*** the new program while it loads[1]"). Just because one limitation requires monitoring, Defendants are incorrect in assuming another claim limitation, where the new program is validated, requires no monitoring. Defendants concede that "[t]he intrinsic evidence only describes ***not requiring*** monitoring of validated programs," meaning that validated programs ***can*** still be monitored, but it is not required. Dkt. 259 at 5. That

[1] All emphases in this brief were added unless otherwise noted.

is not consistent with Defendants' proposed construction that "if the new program is validated, then it is ***not monitored***."

3. "an execution module coupled to the detection module and operable for monitoring, at the operating system kernel of the computing device, the program in response to the trigger intercepted by the detection module" (Claim 1, '137 Patent)

Defendants incorrectly argue that Fig. 6 is not linked to the claimed "execution module." Claim 1 describes four modules: a pre-execution module, a validation module, a detection module, and an execution module. Figs. 4A and 4B are titled "Pre-Execution Process." Fig. 5 is titled "Validating the Executable," Fig. 7 is titled "Trigger of Detect Drivers,"[2] and Fig. 6 is titled "Non-Validated Execution Process." It is no coincidence that the claimed modules and each of the Figures correspond to each other. The claimed execution module conducts an execution process after the pre-execution process conducted by the pre-execution module and the validation module cannot validate the executable, in exactly the way that Fig. 6 is described in the specification: "[T]he exemplary processes illustrated in FIG. 6 and FIG. 7 occur after the pre-execution process and concern executable files that the binary execution monitor 125 could not validate in the pre-execution phase. Referring to FIG. 6, an exemplary process 600 is illustrated for executing an executable file that has not been validated." Ex. B, 9:38-43.

Defendants' rehashing of their arguments for the previous disputed claim term should be disregarded because categorizing Claim 1 as a binary determination between "monitoring" versus "not monitoring" is incorrect. There is a binary determination in Claim 1, but it is between whether a program is validated in the pre-execution process/module and does not need to proceed through the execution process/module, and whether a program is not validated and does need to proceed

[2] The '137 Patent specification is clear that Fig. 7 refers to the detection module. Ex. B, 10:16-17 ("Referring to FIG. 7, ***an exemplary detection process*** 645 is illustrated that employs the file input/output detector 160.").

through the execution process/module. *See* Ex. B, 8:28-39.

4. "network administration traffic" (Claims 1-2, 9-10, 13-14, and 17-18, '356 Patent); "[third/fourth] program instructions to determine if the packet is network administration traffic" (Claims 1, 9-10, 13, and 17, '356 Patent)

a. "Network Administration Traffic" Does Not Require Specific Content

Defendants' diversion as to whether Taasera needs to explain the specific content of the network administration traffic should be ignored. If an administrator sends traffic on the network, there is network administration traffic. The '356 Patent specification describes how network administration traffic is presumed to be harmless because "[s]ome or all bona fide network administrators are known to the administrator of intranet 14 by their combinations of IP protocol and respective IP address." Ex. C, 8:21-29. The exact content or protocol used by an administrator is irrelevant in determining whether traffic is network administration traffic. For example, traffic is not network administration traffic merely because it is SSH traffic (as Defendants suggest), but SSH traffic is network administration traffic when "the protocol[] used by a network administrator [is] SSH and Tellnet.)." *Id.*; *see also* Ex. C, 5:54-59. Put simply, if traffic is sent from a known administrator (all bona fide network administrators are known), it is network administration traffic.

b. Fig. 7 Adequately Discloses the Claimed Algorithm of "[third/fourth] program instructions . . ."

Defendants seem to agree with Taasera that Fig. 7 is a flowchart linked to the determination of whether the packet is network administration traffic but argue that "Figure 7 is not 'adequate structure'" because it does not describe how "to determine if traffic is [] SSH or VNC traffic." Dkt. 259, at 8. As noted above, the patent specification describes common "examples of network administration traffic" from a network administrator, such as "remotely install[ing] a patch or chang[ing] configuration" or "remotely add[ing] a userID," which could be SSH or VNC traffic. Ex. C, 5:54-59. Whether the traffic is SSH or VNC is irrelevant as to whether the traffic is network administration traffic because not every SSH or VNC traffic is network administration traffic.

The proper inquiry of whether the algorithm of Fig. 7 provides adequate structure is not whether it discloses structure for specifically determining whether traffic is SSH or VNC but whether it adequately defines the bounds of the claim: "determin[ing] if the packet is network administration traffic." *Alfred E. Mann Found. for Sci. Rsch. v. Cochlear Corp.*, 841 F.3d 1334, 1341–42 (Fed. Cir. 2016) ("In software cases, therefore, algorithms in the specification need only disclose adequate defining structure to render the bounds of the claim understandable to one of ordinary skill in the art.") (citing *AllVoice Computing PLC v. Nuance Commc'ns, Inc.*, 504 F.3d 1236, 1245 (Fed. Cir. 2007); *Ergo Licensing, LLC v. CareFusion 303, Inc.*, 673 F.3d 1361, 1365 (Fed. Cir. 2012) ("An algorithm may be expressed 'in any understandable terms including as a mathematical formula, in prose, or as a flow chart, or in any other manner that provides sufficient structure.'") (citations omitted). The algorithm disclosed in Fig. 7 meets this burden, which Defendants do not dispute under this standard.

5. "attestation" (Claims 1-3, 5, and 7, '441 Patent; Claim 1, '616 Patent)

Defendants' arguments still do not address why extra clarification is necessary beyond "verification." For example, Claim 1 of the '441 Patent explicitly states "[a] method of providing an ***attestation service*** for an ***application***…" and Claim 1 of the '616 Patent explicitly states "[a] method of providing an ***attestation service*** providing runtime operational integrity ***of a system***." In view of the redundancy, Defendants' proposed constructions should be rejected.

6. "[at] runtime" (Claim 1, '616 Patent)

Defendants' only argument is that their construction is supported by both the parties' agreements for other patents. Dkt. 259 at 12. But the only relation between the four patents in question (the '517, '441, '948, and '616 Patents) is that the '616 Patent and '948 Patent share the same priority date. And the claims between the '616 Patent and '948 Ppatent are different. The

’948 Patent, Claim 1 claims “a ***runtime configuration of the application***” but the ’616 Patent, Claim 1 claims “sending, by the endpoint trust agent on a monitored device, a dynamic context including endpoint events and actions of the monitored device and applications executing on the monitored ***device at runtime***.” Given that the patents have the same inventors and same priority date, this difference must be presumed as intentional. *CAE Screenplates v. Heinrich Fiedler GmbH & Co.*, 224 F. 3d 1308, 1317 (Fed. Cir. 2000) (“In the absence of any evidence to the contrary, we must presume that the use of these different terms in the claims connotes different meanings.”).

Further, Defendants’ proposed construction of “the application being monitored” is wrong. Claim 1 of the ’616 Patent claims “the monitored device at runtime.” The specification confirms monitoring a running device. *See* Ex. J, 22:21-23 (“an integrity processor ***630 on a device 560, for runtime*** system 1016, application 1015 and user 1014 context”). Defendants’ other argument that “Plaintiff’s proposed construction renders ‘at runtime’ a nullity” because “devices must necessarily be running in order to send or receive information” is also incorrect because there may be multiple devices or endpoints on a network. *See* Ex. J, 22:43-44 (“In an embodiment, the network endpoint assessment 1001 comprises performing a security scan of ***network endpoints*****”**). Some of those network endpoint devices may be running while others are not, which is why Claim 1 specifies “the monitored device at runtime.”

7. “a computing platform comprising a network trust agent” (Claim 1, ’616 Patent)

Defendants do not engage with the arguments presented in Taasera’s Opening Brief that Defendants clearly understand an “endpoint trust agent” without a construction and, therefore, understand “trust agent” without any construction. The modifier “endpoint” or “network” merely denotes the location of the “trust agent,” as confirmed by the specification and Fig. 12 of the ’948 Patent, which Defendants do not dispute. *See* Dkt. 256 at 14-16.

8. "at runtime receiving . . . a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded components of the application" (Claims 1 and 4, '441 Patent)

Defendants' construction restates the claim limitation with a few distinctions. The first distinction relates to its interpretation of the claimed "runtime" as "at the time the relevant program is running." This dispute is described above. *See supra* Section I.6. The second distinction is completely negating the claimed "wherein the attributes comprise one or more . . . ," which alone is reason to reject Defendants' proposed construction. The third distinction is construing the claimed "executable file binaries of the application" as "the executable file binaries of the application (as distinct from binary hashes)." If "the plain language shows that executable file binaries and binary hashes are different," as Defendants allege, then no construction is necessary. Yet, it is Defendants who are asserting the distinction based on incorrectly reading one sentence in the prosecution history. The total statement during prosecution highlights the apples-to-oranges comparison between Starnes and the claim language: "As discussed during the interview, ***verifying an application state on a given device based upon comparing the results of a scheduled scan of binary hashes and loadable modules to a set checklist is not analogous to 'attributes of the application at runtime comprising executable file binaries and loaded components of the application***.'" Ex. S at 23. Read properly, the prosecution history clarifies that comparing scan results to a checklist is not the same as receiving one or more executable file binaries of the application and loaded components. This has nothing to do with whether executable file binaries are distinct from binary hashes. Defendants' cited portions of the specification are also inapposite because they merely cite to instances of mentioning "executable file binaries" and "hash."

9. "a security context providing security information about the application" (Claims 1 and 4-5, '441 Patent)

Defendants argue that "the claims recite what the 'security context' does, and how it is used by the 'attestation server' after it is received, but not what the 'security context' *is*." Dkt. 259 at 16. But that is wrong and undermined by Defendants' repetition of claim language in its proposed construction. Claim 1 provides a full understanding of a security context that abrogates the need for any construction outside the plain and ordinary meaning: "a security context providing security information about the application, wherein the security information comprises an execution analysis of the one or more executable file binaries and the loaded components." Defendants do not address Taasera's Opening Brief, which argues that adding "collaboration services" to the proposed construction is improper based on principles of claim differentiation and the specification describing collaboration services as an exemplary embodiment. Dkt. 256 at 19.

10. "an application artifact" (Claim 2, '441 Patent)

Defendants argue that a construction is required because "what 'an application artifact' *is* remains unclear when reading the claims" (Dkt. 259 at 18), and then proceeds to ignore Claim 2 of the '441 Patent, which defines "an application artifact as a reference for ***changes in a subsequent*** execution context," and not data that describes the application runtime context. Defendants also ignore Taasera's argument that Defendants' construction, based on only one exemplary embodiment, improperly narrows the claim limitation to the exclusion of embodiments elsewhere in the specification showing that application artifacts can be "record[s] of the state of the discovered or identified applications running on the instrumented platform 100). *Id.*, 7:27-32.

11. "introspective security context" (Claims 4 and 5, '441 Patent)

Defendants' argument that Ex. D, 9:47-54 is not referring to introspection based security contexts is wrong. The specification starts by pointing out that an "attestation broker 109 may request introspection based security context . . . for the running application . . . from one or more of the plurality of collaborative services 110." Ex. D, 9:40-46. Because the introspection based security context is requested from collaboration services, it follows that the directly subsequent description of collaboration services performing just-in-time inspection, is an introspection based security context. *Id.*, 9:47-54. This example does not involve "sampl[ing] over a period of time" because it is a "lookup [of] the most recent inspection report," rendering Defendants' proposed construction directly contrary to the specification and incorrect. *Id.*

12. "the application of the restriction on the user's transaction" (Claim 11, '441 Patent)

The parties' dispute is whether Claim 11 depends upon Claim 9 or Claim 10, and whether there is reasonable debate on that point. There is none. Claim 10 refers to "restrict[ing] [] the user's network access to the application." Claim 11 "rout[es] decisions and redirect[s] the user to an alternate computer platform," which requires network access. Ex. D, 6:65-7:12 ("Referring to FIG. 1, ***the exemplary network*** 150 may include . . . an attestation broker 109 that may receive a request to attest to the identify [sic] of a running application . . . ***The application may be an application targeted for use by an access requestor 114 (e.g., another computing platform***)." Claims 10 and 11 are mutually exclusive and Claim 11 must derive antecedent basis from Claim 9.

13. "return URL" (Claims 1, 3-4, 6-7, 9-10, 12-13, 15-16, and 19, '419 Patent; Claims 1, 3-6, and 8, '634 Patent; Claims 1-6 and 8-10, '251 Patent; and Claims 1, 5-6, 10-12, and 16-18, '453 Patent)

Defendants insist that a URL ***must*** be encrypted to form a new URL when it is returned to the browser. But this is wrong. There can be no conflation of the URL with the resource when Claim 1 of the '419 Patent itself claims "determining, by the computer, ***whether encryption is required for none, part, or all of a return URL***. Defendants also refuse to engage with the specification: "If the resource is to be ***returned without a URL change***, then the process moved to step 62. The resource is returned to the requesting browser 51. Otherwise, ***if the URL must be encrypted***, the process moves to step 58. Ex. E, 6:64-7:4. Defendants also do not address that, outside of "a new URL," the remainder of their construction is redundant over the language of the claim limitation. *See id.*, Claim 1.

14. "evaluating[, by the computer,] the URL to determine whether encryption of [none, part, or all of] the URL is required" (Claims 1, 4, 10, 13, and 17, '419 Patent; Claims 1 and 4, '634 Patent); "determining, by the computer, whether encryption is required for none, part, or all of a return URL" / "determining[, by the computer,] [whether/that] encryption of [a/the] return URL [of the requested resource] is required" / "determining by the computer, [whether/that] encryption of the contained URL [is/is not] required" / "determine that encryption of the URL is not required" (Claims 1, 4, 13, and 19, '419 Patent; Claims 1 and 4, '634 Patent; Claims 1-6 and 8-10, '251 Patent; Claims 1, 4, and 6-18, '453 Patent)

Instead of engaging with Taasera's Opening Brief arguments, Defendants opt to improperly provide a non-infringement argument based on Taasera's infringement contentions. Dkt. 259 at 37. This should be ignored.

Defendants' other argument does not show how replacing the claimed "determining" / "evaluating" with "deciding" adds any understanding to the claim limitations as written and is otherwise nonsensical. Defendants argue that:

> ['251 Patent Claim 1] requires 'determining, by the computer, that encryption of the contained URL is required **and in response, calculating, the by** [sic] **computer, an encrypted value**'[3] of the URL. Thus, this language is deciding whether the request URL needs to be encrypted, and encrypting it if so. It is not simply checking to see if the URL is already encrypted.

Id. (citing '251 Patent, Claim 1) (citations omitted). At most, Defendant is indicating that, because the claim language in the '251 Patent provides a calculation in response to determining whether encryption is required, "determining" should be construed as "deciding" and "not simply checking." But the claim language in each of the four patents is clear enough that the "determining" or "evaluating" is not "checking" if the URL is encrypted already, without having to construe it as "deciding." Defendants ignore that both of their proposed substitutions of the claim language, "deciding," and "should be performed," are nowhere in the '419, '634, '251, or '453 Patent

[3] The limitation "and in response, calculating, by the computer, an encrypted value" is only in the '251 Patent.

specifications. It remains unclear as to how a POSITA would gain some greater understanding of the claim language from Defendants' proposed substitutions.

15. "determining whether encryption of none, part, or all of a return URL of the requested resource that is to be returned to a location of the resource request" (Claim 10, '419 Patent)

Claim 10 is a computer program analogue to Claim 1. The analogous claim limitation of Claim 1 states: "determining, by the computer, whether encryption is required for none, part, or all of a return URL of the requested resource that is to be returned to a location of the resource request." Given Defendants' clarification about their indefiniteness argument, the obvious minor typographical error correction for this limitation of Claim 10 is as follows: determining whether encryption is required for ~~of~~ none, part, or all of a return URL of the requested resource that is to be returned to a location of the resource request."

16. "determining[, by the computer,] whether the URL of the requested resource is required" (Claims 2 and 11, '419 Patent; Claim 2, '634 Patent)

Defendants argue that the wording of this claim limitation, as well as that of the specification, is "not coherent English." Dkt. 259 at 40. But the scope of this claim limitation is not complicated. The claim language unambiguously recites that a URL is associated with a resource (*i.e.*, the URL of the requested resource). If the resource will be returned to a requestor, the computer determines that "the URL of the requested resource is required," as the claim limitation spells out. If the resource cannot be returned to a requestor, then the computer determines that the URL of the requested resource is not required. *See* Ex. E*,* 7:9-18. This claim limitation requires determining, by the computer, whether the URL is required or not. Nothing more.

17. "compliance state of the endpoint" (Claims 1, 12, and 23, '038 Patent; Claims 1, 11, and 21, '997 Patent; Claims 1, 9, and 17, '918 Patent)

Defendants argue that the claim language states what the "'compliance state' is 'based on';

not what the 'compliance state' *is*." Dkt. 259 at 43. But Defendants do not construe "compliance" or "endpoint." The claim language is clear that the compliance state is the result of a comparison of "status information" (*i.e.*, a state of the endpoint) and "compliance policies." '038 Patent, Claims 1, 12, and 23; '997 Patent, Claims 1, 11, and 21; '918 Patent, Claims 1, 9, and 17. Defendants also attempt to relate compliance scores with policy thresholds, neglecting other disclosed embodiments (*e.g.*, data source relative weightings, attribute relative weightings, etc.). *See* Ex. G, 39:30–34; Ex. L, 40:1–5; Ex. O, 39:46–50. Defendants' unnecessary limiting of the claims based on the specification should be rejected.

18. "compliance polic[y/ies]" (Claims 1, 12, and 23, '038 Patent; Claims 1, 11, and 21, '997 Patent; Claims 1, 9, and 17, '918 Patent)

Notably, for the previous term, Defendants have no construction issue for "compliance policy" and include it in their proposed construction. Defendants also do not address Taasera's argument that Defendants' proposed construction improperly limits "compliance policies" to the examples provided in the specification, even where the specification contemplates additional categories of values through use of "etc.," as noted below:

> Different sets of compliance policies may have the same or different values regarding items monitored, compliance thresholds, analysis methods to use, ***etc.***"

Ex. G, 56:51-63; Ex. L, 58:6–19; Ex. O, 57:45–57. Defendants' proposed construction that compliance policies are the "items on an endpoint to monitor, the analysis methods to use, and the permitted thresholds," based on the cited portion above, is also improper. The cited portion states that "compliance policies ***may have the same or different values regarding*** items monitored…" not that they are "items monitored," "analysis methods," or "thresholds" themselves.

19. "real-time" / "real time" (Claims 1 and 2, '948 Patent)

Taasera now construes "real-time" / "real time" according to its plain and ordinary meaning which, as Defendants argue, is evident from the specification and surrounding claim language.

Dkt. 259 at 28. Notably the word "immediate" is absent from the '948 Patent specification and would not add to a POSITA's understanding of the claim term.

20. "substantially real time"/ "substantially real-time data" (Claims 1, 10, and 17, '518 Patent)

Defendants' disagreement stems from an alleged failure to "identify any 'objective boundaries.'" Dkt. 259 at 31. But the specification clearly discloses that the metes and bounds of this claim limitation are the various processing limitations of the system.

Claim 1 recites "status information for each mobile device is gathered from a plurality of sources including each mobile device in a substantially real time manner." The specification explains that message handlers are intended to provide real-time status updates. However, between the combination of message handlers "processing mobile device status information," and the device database "updat[ing] these records" by comparing old status information to incoming status updates, the device database can only "provide substantially real-time information about the status of mobile devices" to the server, which gathers the status information.

> Upon processing mobile device status information, message handlers 18 provide real-time status updates 22 to be stored and organized as records in device database 20
> …
> Using status updates 22, device database 20 can update these records and provide substantially real-time information about the status of mobile devices 10
> …
> Furthermore, old status information in device database 20 can be compared to incoming status updates 22 to determine which attributes of a mobile device have changed on a substantially real-time basis. Accordingly, device database 20 can maintain status information about mobile devices enrolled with the MDM system as a series of device attributes that are updated on a substantially real-time basis.

Ex. I, 10:44–65.

The specification also describes why there would be an unintentional delay in the context of gathering "status information for each mobile device." Actions affect the status of a device, and when status information updates for a device are sent to maintain a record of actions and compliance state changes of the device due to those actions, "there may be a delay" in actual completion of the action that was intended to be in real-time, and thus an unintentional delay in gathered status information.

> Upon evaluation of the rules by core rules engine 28, device database 20 may be updated to reflect any changes in the compliance status of the mobile device…Core rules engine 28 may send status updates 32 to device database 20 to maintain a record of actions and compliance state changes of the device. In some embodiments, there may be a delay between action requests 30 and the actual completion of the action by the action execution controller 34. For example, if a device is off-line, it may be several hours or days before an action could be completed.

Ex. I, 12:64–13:9. One non-limiting example given of processing limitation, as described above, is whether a device is offline. Dr. Cole describes that there are several other processing limitations that a POSITA would understand to cause an unintentional delay between real-time and substantially real-time, such as high traffic on the mobile network and transmission delays. *See also* Ex. P, ¶¶ 79-80. While "substantially" is a term of degree, the patent specification is clear on its objective boundaries.

21. "which includes a network analyzer, an integrity processor, an event correlation matrix, a risk correlation matrix, and a trust supervisor" (Claim 1, '948 Patent)

Defendants' indefiniteness argument hinges on incorrectly asserting that "the '948 Patent's specification . . . [does not] provide[] a definition of the an "integrity processor" or a "trust supervisor." Dkt. 259 at 21. Yet, the specification has clearly labeled sections for each of these components. The "Integrity Processor" is titled and described on Ex. H, 17:16-34 and the "Trust Supervisor" is titled and described in detail on Ex. H, 22:26-24:67.

22. "operational integrity of the application" (Claim 1, '948 Patent)

Defendants' construction improperly seeks to define "operational integrity" as "the level of threat or contextual worthiness" based on language from the Abstract alone. *Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1121 (Fed. Cir. 2004) ("While a statement in the Abstract may operate as a clear expression of manifest exclusion, for several reasons, this statement does not. Nor does this statement weigh heavily when considering whether the applicant has acted as his own lexicographer. To begin, this statement is in the Abstract of the patent. This section of a patent speaks generally to the invention and, much like the syllabus of an opinion, sets forth general information about the document's content, which is described in more detail in the remainder of the document."). Defendants also do not address Taasera's argument concerning why narrowing the claim term based on the Abstract would be more appropriate than the plain and ordinary meaning of the claim term given the context of a full section in the specification titled "System for Evaluating Operational Integrity of Applications" Ex. H at 12:55-63. Therefore, "operational integrity of the application" would readily be understood under its plain meaning given the plentiful context of the patent specification without Defendants' narrowing construction.

23. "an event correlation matrix" (Claim 1, '948 Patent)

Defendants continue to ignore that their construction is based on descriptions of Figs. 6, 7A, and 7C, which are each referred to as "an exemplary embodiment of the present disclosure." *Id.*, 6:43-53. The plain and ordinary meaning should be applied. Separately, Defendants' proposed construction adds no further understanding to what a POSITA would receive from reading the specification because Defendants merely construe "correlation" as "map[ping]" and otherwise use "event" and "matrix" in its proposed construction.

24. "a risk correlation matrix" (Claim 1, '948 Patent)

Similar to the "event correlation matrix" term above, Defendants improperly rely on descriptions of Figures 4-7, where the "risk correlation matrix" is "***embodied*** as grids." Ex. H, 12:46-54. Again, Defendants' proposed construction adds no further understanding to what a

POSITA would receive from reading the specification because Defendants merely construe "correlation" as "map[ping]" and otherwise use "event" and "matrix" in its proposed construction.

25. "correlating, by the event and risk correlation matrix" (Claim 1, '948 Patent)

Defendants' arguments confirm that their indefiniteness challenge can only be due to willful ignorance of the other claim limitations of Claim 1, namely, ". . . the native computing environment which includes . . . an event correlation matrix [and] a risk correlation matrix…" This previous element of Claim 1 is clear that both the "event correlation matrix" and the "risk correlation matrix" perform the correlation of threat classifications.

26. "initiating… at least one action" / "initiate an action" (Claims 1, 10, and 17, '518 Patent)

Defendants' construction of "initiating" as including "automatically" is redundant to Claims 10 and 17 which already claim "automatically initiating" and "automatically initiate," respectively. With respect to Claim 1, the lack of "automatically" in the claim language when compared to Claims 10 and 17 is intentional because Claim 1 recites "initiating, at the server, at least one action defined by the administrator-defined rules in response to the step of evaluating, wherein the step of evaluating is performed by the server automatically." Unlike Claims 10 and 17, the embodiment disclosed by Claim 1 performs the evaluation automatically and initiates an action in response to the automatic evaluation. *See* Ex. I, 2:23-35 (discussing an embodiment initiating in response to automatic evaluation, in contrast with a separate embodiment disclosed in 2:56-3:2, which discloses automatically initiating). The remainder of Defendants' proposed construction, "causing to begin in real time" is not found in the specification and is otherwise not required to understand the claimed "initiating."

II. CONCLUSION

For all the foregoing reasons, Taasera respectfully requests that the Court adopt Taasera's proposed constructions.

Dated: August 25, 2023

Respectfully submitted,

/s/ Alfred R. Fabricant
Alfred R. Fabricant
NY Bar No. 2219392
Email: ffabricant@fabricantllp.com
Peter Lambrianakos
NY Bar No. 2894392
Email: plambrianakos@fabricantllp.com
Vincent J. Rubino, III
NY Bar No. 4557435
Email: vrubino@fabricantllp.com
Joseph M. Mercadante
NY Bar No. 4784930
Email: jmercadante@fabricantllp.com
FABRICANT LLP
411 Theodore Fremd Avenue,
Suite 206 South
Rye, New York 10580
Telephone: (212) 257-5797
Facsimile: (212) 257-5796

Samuel F. Baxter
State Bar No. 01938000
Email: sbaxter@mckoolsmith.com
Jennifer L. Truelove
State Bar No. 24012906
Email: jtruelove@mckoolsmith.com
MCKOOL SMITH, P.C.
104 E. Houston Street, Suite 300
Marshall, Texas 75670
Telephone: (903) 923-9000
Facsimile: (903) 923-9099

ATTORNEYS FOR PLAINTIFF
TAASERA LICENSING LLC

CERTIFICATE OF SERVICE

The undersigned hereby certifies that all counsel of record who are deemed to have consented to electronic service are being served with a copy of this document via the Court's CM/ECF system per Local Rule CV-5(a)(3) on August 25, 2023.

/s/ Alfred R. Fabricant
Alfred R. Fabricant